Methods to Determine the Primitive Roots of a Number.

By G. A. Miller.

The present note aims to exhibit some elementary relations between well-known methods of finding the primitive roots of a number and the properties of the cyclic group. Incidentally we arrive at a fundamental theorem relating to the primitive roots of a special class of numbers. A corollary of this theorem gives the primitive roots of all the prime numbers of the form $2p+1$, p being a prime, while it has been customary in the works on the theory of numbers to devote two theorems to the primitive roots of such prime numbers.* The note has close contact with the paper published in this JOURNAL under the title "Some Relations between Number Theory and Group Theory" and may be regarded as a continuation of this article.†

It is known that the necessary and sufficient condition that a number g has primitive roots is that the cyclic group G of order g has a cyclic group of isomorphisms I. The numbers which are less than g and prime to it may be made to correspond to the operators of I, unity corresponding to the identity, in such a way that I and the group formed by these numbers, when they are combined by multiplication and the products reduced with respect to modulus g, are simply isomorphic. The orders of the operators of I are the indices of the exponents to which the corresponding numbers belong. In particular, $g-1$ corresponds to the operator of order 2 and the primitive roots of g correspond to the operators of highest order in I. Hence the method of finding the primitive roots of a number is equivalent to that of finding the operators of highest order in a cyclic group.

One of the most instructive methods for finding all the primitive roots of g is analogous to the method known as the "Sieve of Eratosthenes" for finding

* Cf. Cahen, "Éléments de la Théorie des Nombres," 1900, p. 336; Tschebyscheff, "Elemente der Zahlentheorie," 1902, p. 307; Pascal, "Repertorium der höheren Mathematik," Vol. I (1900), p. 530.

† AMERICAN JOURNAL OF MATHEMATICS, Vol. XXVII (1905), p. 315.

the prime numbers which are less than a given number. While there is no general non-tentative method for finding the primitive roots of g, there are general non-tentative methods for finding all the numbers which are less than g and non-primitive roots of g. In group-theory language one of these may be stated as follows: Let p be any prime divisor of g and raise each operator of G to the pth power. These powers are composed of all the operators of G whose orders are not divisible by the highest power of p which divides g. Hence we may obtain all the operators of G which are not of highest order by raising successively all its operators to the powers whose indices are the different prime divisors of g. The remaining operators are of highest order and hence correspond to the primitive roots in I. This method has the advantage that it gives all the primitive roots of g at the same time. Its chief defect is that the same non-primitive root is generally found more than once. From the known congruence $k^2 = (g - k)^2 \bmod g$, it follows that we need to square only half the numbers less than g and prime to g. In particular, when g is a prime number of the form $2^\alpha + 1$ its non-primitive roots are given by l^2, $l = 1, 2, \ldots, 2^{\alpha-1}$. The remaining numbers less than 2^α are its primitive roots.

The most practical general tentative method for finding the primitive roots is based, in group-theory language, upon the fact that the order of the product of two commutative operators is divisible by the highest power of any prime p which divides either one of their orders, provided these orders do not involve the same highest power of p. If we have two commutative operators, we can there fore readily find an operator whose order is the least common multiple of their orders; for, if they should involve the same highest power of p, one of them may be raised to the pth power and thus we can obtain two operators not involving the same highest power of the same prime; and hence the order of their product will be the least common multiple of their orders. When g is not very large, this method generally leads to an operator of highest order in I, or to a primitive root of g, with a few trials. Since all the operators of highest order in any cyclic group may be obtained by raising any one of them to the powers whose indices are prime to this order, all the primitive roots of g may be obtained from any one of them in the same manner.

We are now in position to give a simple proof of the theorem mentioned in the first paragraph. Suppose that the order of I is of the form $2q$, q being any odd prime. Since a square can not correspond to an operator of highest order in I (the order of I being always even) and since α^2, α being any integer prime

to g, can not correspond to the operator of order 2, it follows that α^2 corresponds to an operator of order q whenever $g-1>\alpha>1$. The product of the operator which corresponds to α^2 and the one which corresponds to $g-1$ is of order $2q$, and hence $-\alpha^2$ is a primitive root of g. This result leads directly to the

THEOREM: *When the exponent to which the primitive roots of a given number g belong is of the form $2q$, q being an odd prime, then each of the primitive roots of g is given once and only once by $-\alpha^2$, $1<\alpha<g/2$ and α being prime to g; moreover, α^2 belongs to exponent q.*

COROLLARY: *Every prime of the form $2q+1$, q being an odd prime, has for its primitive roots $-\alpha^2$, $1<\alpha<q+1$. In particular, -4 is a primitive root of every prime of this form.*

It should be observed that the group-theory language employed in the proof of this theorem is not essential, as the results follow directly from the facts that a square can not be a primitive root of any number and that -1 belongs to exponent 2 with respect to any modulus. The forms of the numbers which have primitive roots are assumed to be known throughout the present note. The preceding theorem furnishes the numbers belonging to every possible exponent when g has the required form. It is also clear that the order of I can not be of the form $2q$ unless g is an odd prime, twice an odd prime, 9 or 18.

We may add that some of the known developments in regard to the properties of primitive roots, especially those relating to products, follow directly from the isomorphism between I and the numbers which are less than g and prime to g. For instance, the theorem which affirms that the product of all the primitive roots of a number is congruent to unity whenever the number has more than one primitive root, is included in the evident statement that the continued product of all the operators of the same order >2 in any Abelian group is the identity, since these operators may be arranged in pairs consisting of an operatar and its inverse. The product of all the operators of order 2 in such a group is also known to be the identity whenever the group contains more than one such operator.*

* *Annals of Mathematics*, Vol. IV (1903), p. 188.